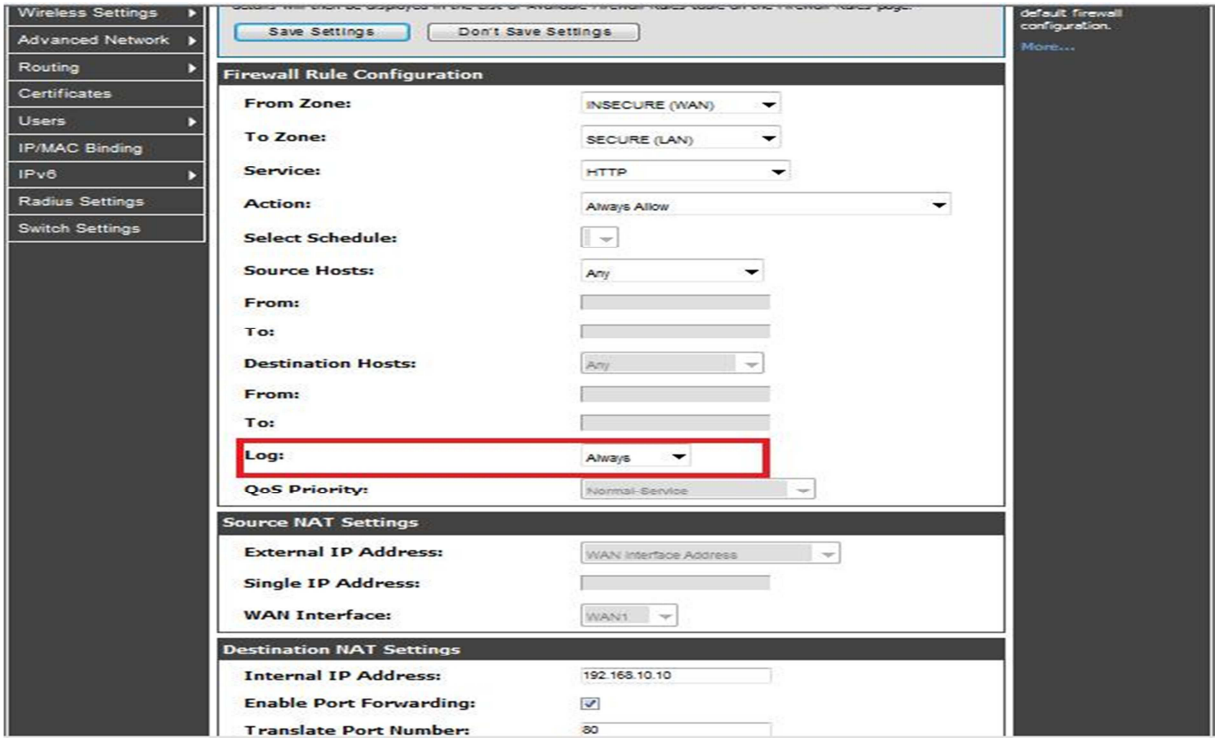
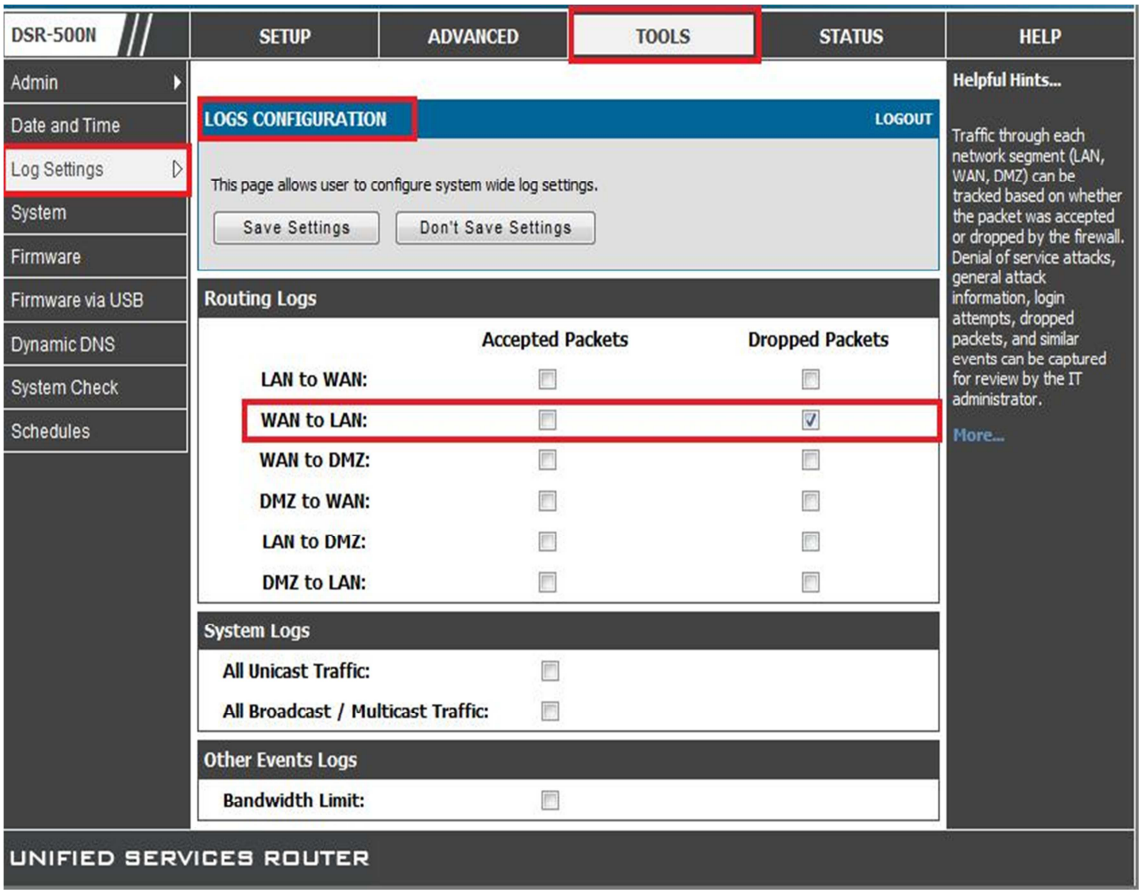
How to setup logging in DSR series

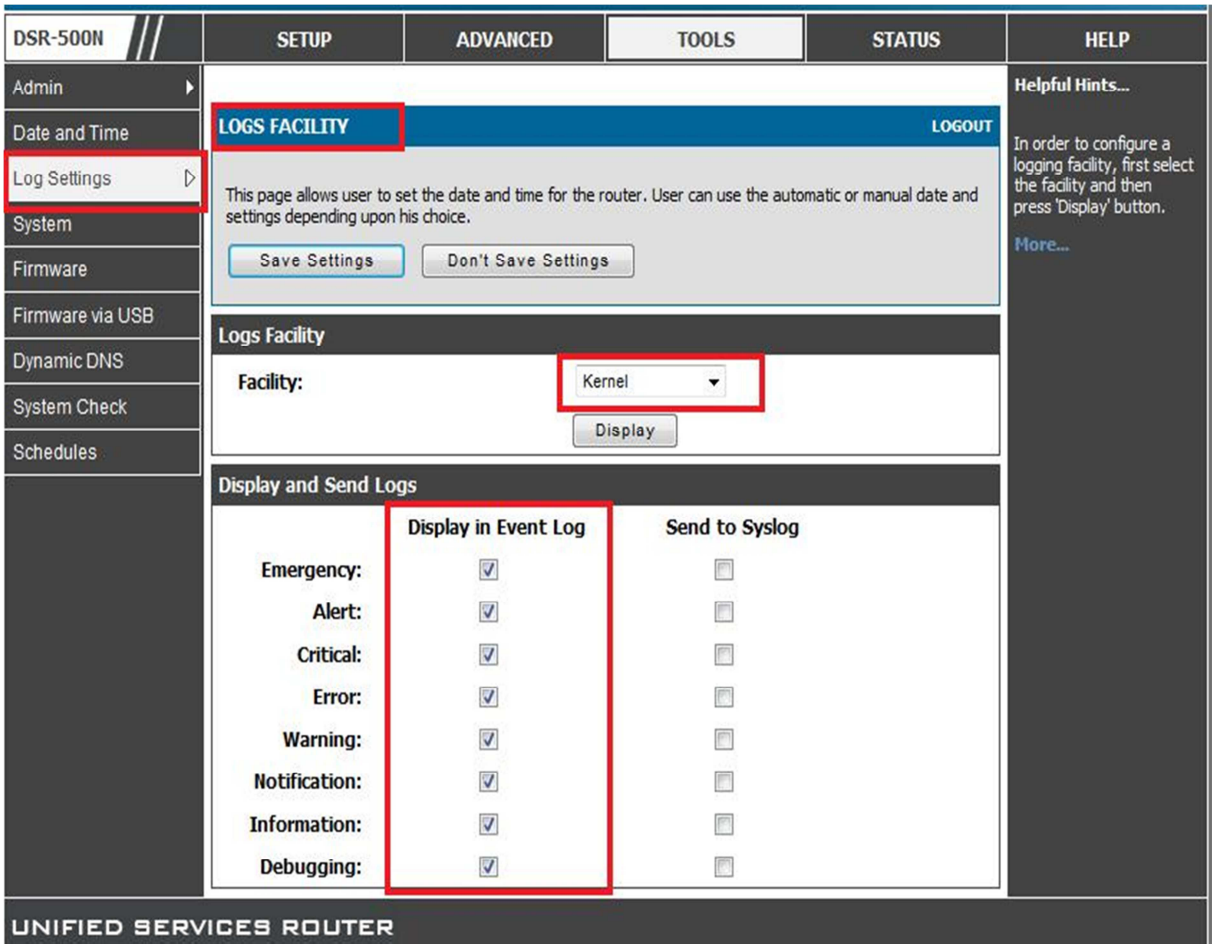
Step1: Make sure the rule that you want to log is enable, we use the firewall rule for example. In the **Log** field, make sure your select **Always**.



Step 2.Under the **TOOLS**->**Log Settings**-> **LOG CONFIGURATION**, select the direction and dropped/accesspt packet you want to log.



Step3:Under **TOOLS**->**Log Settings**-> **LOGS FACILITY**, select the Log Facility and the severity of log want to displays.



You can refer the following for more detail:

Logs Facility:
Facility: There are three core components to the router's firmware and the granularity of logging within each can be set independently. Choose between Kernel, System, and Local-0 Wireless.

Kernel: This covers log messages that correspond to the Linux kernel such as logs generated by firewall or network stack traffic.

System: This covers application and management level features such as SSL VPN or administrator changes for managing the unit.

Display and Send Logs
Each of the following type of logs can be sent to the **Event Log** viewer in the GUI and/or the **Syslog server** configured to capture remote logging.

When a particular severity level is selected, all events with severity equal to and greater than the chosen severity are captured. The severity levels available for logging are:

EMERGENCY: system is unusable
ALERT: action must be taken immediately
CRITICAL: critical conditions
ERROR: error conditions
WARNING: warning conditions
NOTIFICATION: normal but significant condition
INFORMATION: informational
DEBUGGING: debug-level messages